PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-331166
(43)Date of publication of application : 30.11.2000

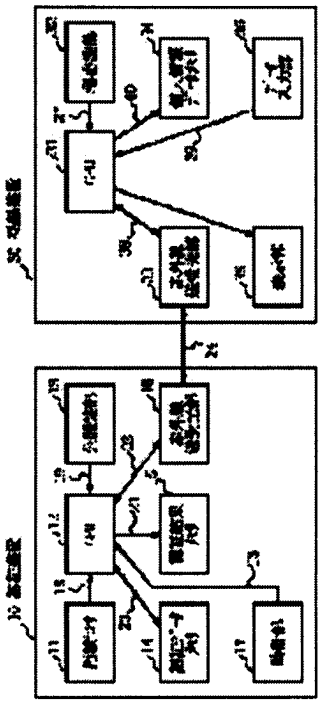
(51)Int.Cl. G06T 7/00
H04L 9/32

(21)Application number : 11-143578
(22)Date of filing : 24.05.1999

(71)Applicant : NEC YONEZAWA LTD
(72)Inventor : YAMAZAKI ATSUSHI

(54) FINGER PRINT AUTHENTICATING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a finger print authenticating system where a highly safe simple system constitution is realized which does not allow the disclosure of finger print information.
SOLUTION: In this finger print authenticating system, a finger print sensor 11 detects finger prints and a public key section 13 stores a public key 19 used for encipherment. An authenticating data memory 14 stores authenticating data 20. An authenticating result memory 15 stores collating data 21 and a CPU 12 outputs the collating data 21 and authenticated and registered finger print data 22. A clock section 17 outputs time data 23 and a data inputting section 35 outputs personal information 39. A personal information data memory 34 stores personal information data 40 and a secret key section 32 stores secret keys 37 for encipherment and decoding. A displaying section 36 displays data and a CPU 31 manages and controls a registering device 30 and infrared-ray transmitting and receiving sections 16 and 33 transmit and receive infrared rays 24.



LEGAL STATUS

[Date of request for examination] 26.04.2000
[Date of sending the examiner's decision of rejection] 10.06.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－331166
（P2000－331166A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０	５Ｂ０４３
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	５Ｊ１０４
			６７３Ａ	

審査請求　有　　請求項の数６　ＯＬ　（全 ７ 頁）

(21)出願番号　特願平11－143578

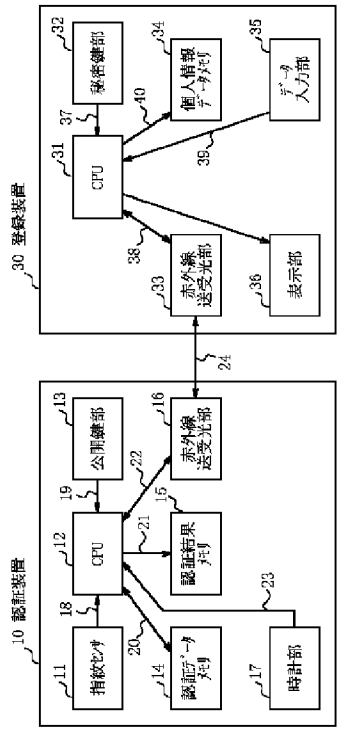
(22)出願日　平成11年５月24日(1999.5.24)

(71)出願人　000240617
米沢日本電気株式会社
山形県米沢市下花沢２丁目６番80号
(72)発明者　山崎　敦
山形県米沢市下花沢２丁目６番80号　米沢日本電気株式会社内
(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5B043 AA01 AA04 BA02 CA08 CA10
FA03 FA07 HA20
5J104 AA07 EA19 GA03 KA01 KA05
KA17 MA02 NA02 NA05 NA36
NA37 NA38 PA10 PA16

(54)【発明の名称】　指紋認証システム

(57)【要約】
【課題】指紋情報を漏洩させない高度な安全性を簡単なシステム構成で実現する指紋認証システムを提供する。
【解決手段】指紋センサ１１は指紋を検出する。公開鍵部１３は暗号化のための公開鍵１９を格納する。認証データメモリ１４は認証データ２０を格納する。認証結果メモリ１５は照合データ２１を格納する。ＣＰＵ１２は照合データ２１および認証登録指紋データ２２を出力する。時計部１７は時刻データ２３を出力する。データ入力部３５は個人情報３９を出力する。個人情報データメモリ３４は個人情報データ４０を格納する。秘密鍵部３２は暗号化および復号化のための秘密鍵３７を格納する。表示部３６はデータを表示する。ＣＰＵ３１は登録装置３０の管理制御を行う。赤外線送受光部１６，３３は赤外光２４を送受する。



【特許請求の範囲】
【請求項１】　指紋情報を暗号化し予め認証登録指紋データとして送信し、指紋照合時に指紋センサデータと、受信及び格納した認証データを復号しこれと比較照合することにより認証を行う認証装置と；前記認証装置から受信した前記認証登録指紋データを復号し、これと個人情報データとから認証データの生成及び暗号化を行い、前記認証データとして送信する登録装置と；を備えたことを特徴とする指紋認証システム。
【請求項２】　前記認証装置が、
指紋を検出し指紋情報を出力する指紋センサと；前記指紋情報の暗号化のための公開鍵を格納する公開鍵部と；前記認証データを格納する認証データメモリと；前記指紋情報と前記認証データとを比較照合した照合データを格納する認証結果メモリと；時刻データを出力する時計部と；前記指紋情報の暗号化、前記認証データの復号化、これらを照合し前記照合データ及び前記認証登録指紋データを出力する第１のマイクロプロセッサと；前記認証登録指紋データの送受を赤外光により行う第１の赤外線送受光部と；を有することを特徴とする請求項１記載の指紋認証システム。
【請求項３】　前記登録装置が、
前記赤外光を送受する第２の赤外線送受光部と；データ入力を行い個人情報を出力するデータ入力部と；前記個人情報データを格納する個人情報データメモリと；暗号化及び復号化のための秘密鍵を格納する秘密鍵部と；データの表示を行う表示部と；復号化した前記認証登録指紋データ及び前記個人情報データから前記認証データを生成し、これを暗号化する第２のマイクロプロセッサと；を有することを特徴とする請求項１又は請求項２記載の指紋認証システム。
【請求項４】　前記認証装置及び前記登録装置間の送受信通信をイーサネット（登録商標）により行うことを特徴とする請求項１、２又は３記載の指紋認証システム。
【請求項５】　前記認証装置が、
第１のマイクロプロセッサと、前記指紋センサと、作業用メモリと、時刻データを出力する時計と、赤外線送受光器と、プログラム及び各種データを記憶する不揮発性メモリと、電源供給の電池と、カバーオープン検出回路とを有することを特徴とする請求項１記載の指紋認証システム。
【請求項６】　前記作業用メモリが、フラッシュ・リード・オンリー・メモリであることを特徴とする請求項５記載の指紋認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は指紋認証システムに関し、特に指紋情報を予め登録した認証データと照合する指紋認証システムに関する。
【０００２】
【従来の技術】一般に、金融機関や防衛施設等では高度なセキュリティ管理が要求されるので、予め登録された人物に対してのみ金融利用や入室等の許可を行う個人指紋認識システムが広く用いられている。
【０００３】個人の指紋パターンは、隆線が分岐する位置と分岐数、終端する位置が個人により異なる特徴を有するので、この特徴を抽出して指紋情報の判定を行うことができる。
【０００４】図４は従来の指紋認証システムを示すブロック図である。
【０００５】従来の指紋認証システムは、指紋を検出する指紋センサ１と、個人情報のデータを入力するデータ入力部４と、個人情報のデータを表示する表示部５と、個人情報のデータを記憶する個人情報データ記憶部３と、データの管理制御を行うＣＰＵ２と、ＣＰＵ２により処理された指紋の照合結果を記憶する認証結果メモリ６とから構成されている。
【０００６】次に動作について説明する。
【０００７】指紋センサ１は指紋を数値データに変換し、指紋データとしてＣＰＵ２に出力する。ＣＰＵ２は、個人情報データ記憶部３に記憶していた指紋データと指紋センサ１から読みとった指紋データとを比較し本人照合を行い、照合結果を認証結果メモり６に格納する。
【０００８】データ入力部４と表示部５は、個人情報の入力と画面表示に使用される。
【０００９】この構成の場合、個人情報を暗号化することも可能であるが、暗号化、復号化に使用する鍵データは、両方とも指紋認証システム内に組み込む必要がある。
【００１０】このような技術の一例として、特開平５－２９０１４９号公報記載の「指紋照合認証方式及びその装置」が知られている。
【００１１】この公報では、指紋照合に用いる指紋情報を暗号化して登録し、かつ照合時にも暗号化したままの状態で照合することで、指紋のオリジナル情報が盗まれたり漏洩することを防止する技術が記載されている。
【００１２】
【発明が解決しようとする課題】上述した従来の指紋認証システムは、個別に個人情報を登録する必要があるため、システム構成が複雑になるという欠点を有している。
【００１３】個人情報が指紋認証システムに格納されているため、指紋認証システムを解析すれば偽装が可能になり指紋情報が漏洩するという欠点を有している。
【００１４】また、個人情報を暗号化して格納する場合でも、暗号化と復号化に使用する鍵は、指紋認証システム内に格納するため、暗号解読が可能であり指紋情報が漏洩するという欠点を有している。
【００１５】本発明の目的は、指紋情報を漏洩させない

高度な安全性を簡単なシステム構成で実現する指紋認証システムを提供することにある。

【００１６】

【課題を解決するための手段】本発明の指紋認証システムは、指紋情報を暗号化し予め認証登録指紋データとして送信し、指紋照合時に指紋センサデータと、受信及び格納した認証データを復号しこれと比較照合することにより認証を行う認証装置と；前記認証装置から受信した前記認証登録指紋データを復号し、これと個人情報データとから認証データの生成及び暗号化を行い、前記認証データとして送信する登録装置と；を備えたことを特徴としている。

【００１７】前記認証装置が、指紋を検出し指紋情報を出力する指紋センサと；前記指紋情報の暗号化のための公開鍵を格納する公開鍵部と；前記認証データを格納する認証データメモリと；前記指紋情報と前記認証データとを比較照合した照合データを格納する認証結果メモリと；時刻データを出力する時計部と；前記指紋情報の暗号化、前記認証データの復号化、これらを照合し前記照合データ及び前記認証登録指紋データを出力する第１のマイクロプロセッサと；前記認証登録指紋データの送受を赤外光により行う第１の赤外線送受光部と；を有することを特徴としている。

【００１８】前記登録装置が、前記赤外光を送受する第２の赤外線送受光部と；データ入力を行い個人情報を出力するデータ入力部と；前記個人情報データを格納する個人情報データメモリと；暗号化及び復号化のための秘密鍵を格納する秘密鍵部と；データの表示を行う表示部と；復号化した前記認証登録指紋データ及び前記個人情報データから前記認証データを生成し、これを暗号化する第２のマイクロプロセッサと；を有することを特徴としている。

【００１９】また、前記認証装置及び前記登録装置間の送受信通信をイーサネットにより行うことを特徴としている。

【００２０】前記認証装置が、第１のマイクロプロセッサと、前記指紋センサと、作業用メモリと、時刻データを出力する時計と、赤外線送受光器と、プログラム及び各種データを記憶する不揮発性メモリと、電源供給の電池と、カバーオープン検出回路とを有することを特徴としている。

【００２１】前記作業用メモリが、フラッシュ・リード・オンリー・メモリであることを特徴としている。

【００２２】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００２３】図１は本発明の指紋認証システムの一つの実施の形態を示すブロック図である。

【００２４】図１に示す本実施の形態は、指紋認証を行う認証装置１０と、指紋データや個人データの登録を行う登録装置３０とから構成されている。

【００２５】認証装置１０は指紋を検出し指紋情報１８を出力する指紋センサ１１と、指紋情報１８の暗号化のための公開鍵１９を格納する公開鍵部１３と、認証データ２０を格納する認証データメモリ１４と、指紋情報１８および認証データ２０を比較照合した照合データ２１を格納する認証結果メモリ１５と、時刻データ２３を出力する時計部１７と、指紋情報１８の暗号化、認証データ２０の復号化、これらを照合し照合データ２１および認証登録指紋データ２２を出力するＣＰＵ１２と、認証登録指紋データ２２の送受を赤外光２４により行う赤外線送受光部１６とを有している。

【００２６】また、登録装置３０は赤外光２４を送受する赤外線送受光部３３と、データ入力を行い個人情報３９を出力するデータ入力部３５と、個人情報データ４０を格納する個人情報データメモリ３４と、暗号化および復号化のための秘密鍵３７を格納する秘密鍵部３２と、データの表示を行う表示部３６と、認証登録指紋データ２２を復号化しこれを個人情報データ４０とから認証データ３８を生成し、暗号化するＣＰＵ３１とを有している。

【００２７】ここで公開鍵、秘密鍵とは数値データであり、生成多項式により生成される暗号データである。一般に、公開鍵で暗号化したデータは秘密鍵でのみ復号化でき、逆に秘密鍵で暗号化されたデータは公開鍵でのみ復号化できる特性を有しているので、漏洩に対する安全性が高い。これら公開鍵、秘密鍵のデータは個別素子に格納されると云うよりは、プログラムメモリの一部に格納される。

【００２８】公開鍵１９、秘密鍵３７を使った暗号化方式の特徴を説明すると、鍵と呼ばれている物は、暗号化、復号化するための数値データである。公開鍵暗号化方式とは、公開鍵で暗号化したデータは秘密鍵でのみ復号化可能で、同様に秘密鍵で暗号化したデータは公開鍵でのみ復号化できる方式を云う。この特徴を利用して、安全にかつ簡単な構成で認証システムが構築可能となる。

【００２９】次に各部の動作を説明する。

【００３０】指紋センサ１１は個人の指紋を数値化し指紋情報１８を出力する。ＣＰＵ１２は認証データメモリ１４が格納する認証データ２０を読み出し、公開鍵１９で復号化した後指紋情報１８と比較し、比較した結果をさらに公開鍵１９で暗号化し、照合データ２１として認証結果メモリ１５に格納する。

【００３１】このとき、時計部１７から得られる時刻データ２３も同時に公開鍵１９で暗号化して認証結果メモリ１５に格納する。認証データ２０の登録は、認証装置１０の赤外線送受光部１６と登録装置３０の赤外線送受光部３３を使って相互に通信することにより行う。

【００３２】まず、データ入力部３５から入力された個

人情報３９を、表示部３６で確認する。同時に、認証装置１０の指紋センサ１１で指紋を読み込ませ、公開鍵部１３に格納された公開鍵１９で暗号化した認証登録指紋データ２２を、赤外線送受光部１６で赤外光２４により登録装置３０へ送信する。

【００３３】登録装置３０は、秘密鍵部３２に格納した秘密鍵３７で復号化し、入力した個人情報３９と認証登録指紋データ２２とを併せてこれらを個人情報データ４０として、個人情報データメモリ３４に格納する。同時に、個人情報３９と認証登録指紋データ２２を基にして認証データ３８を生成し、秘密鍵部３２の秘密鍵３７で暗号化した後、赤外線送受光部３３を使って認証装置１０に送信する。この受信された認証データ３８は、ＣＰＵ１２により処理され認証データ２０として認証データメモリ１４に格納される。

【００３４】図２は本発明の指紋認証システムの動作の一例を示す動作説明図であり、図２（ａ）は認証動作を示し、図２（ｂ）は登録動作を示す。

【００３５】次に、図１および図２（ａ）を参照して本実施の形態の動作をより詳細に説明する。

【００３６】指が指紋センサ１１に置かれると、指紋センサ１１は指の指紋を数値化し指紋情報１８として出力する。

【００３７】ここで指紋の数値化とは、指紋と一対一の数値データに置き換えることを意味するが、人間の指紋のパターン（右巻き、左巻き）と任意の何点かの特徴点とを抽出し、データパターン化している。

【００３８】認証データメモリ１４に格納された認証データ２０を公開鍵１９で復号化し、読みとった指紋情報１８と比較する。比較した照合結果は照合データ２１として、時刻データ２３と共に公開鍵１９で暗号化され認証結果メモリ１５に格納される。なお、入退室システムに利用する場合は、照合結果により扉を開放する。認証結果の記録は、登録装置３０を使って確認できる。

【００３９】次に登録動作を図２（ｂ）を使用して説明する。

【００４０】ここで、認証装置１０と登録装置３０の赤外線送受光部１６，３３が赤外光２４で通信できる状態とする。

【００４１】データ入力部３５を用いて個人情報３９を入力する。同時に、認証装置１０の指紋センサ１１で登録する人の指紋を読み込ませる。認証装置１０側で、公開鍵１９を使い指紋情報１８を暗号化して、登録装置３０に送信する。登録装置３０では指紋情報１８を含む認証登録指紋データ２２を秘密鍵３７で復号化して、入力された個人情報３９と併せて個人情報データメモリ３４に格納する。

【００４２】同時に、認証データ３８を作成し、秘密鍵３７で暗号化し認証装置１０へ送信する。認証装置１０は、認証データ２０を認証データメモリ１４へ格納する。

【００４３】このとき、秘密鍵３７を替えることにより、複数の認証データ３８を生成できる。

【００４４】なお、認証データについて説明すると、登録装置３０に登録されている個人情報データ４０は、個人を識別する情報（例えば、名前、社員番号等）と、個人に対する指紋情報１８と、個人が保有する権利の種別（どの認証システムで認証されるか、例えば入退室システムの場合は入室権）とから構成されている。これに対して、認証装置１０に暗号化されて格納される認証データ２０は、指紋情報１８と、この認証装置１０における権利からのみ構成されているので、たとえ認証データ２０を解析できても、個人を特定することができず、偽装は困難となる。

【００４５】図３は図１に示す認証装置の詳細ブロック図である。

【００４６】なお、図３において図１に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【００４７】図３を参照すると、認証装置１０はＣＰＵ１２と、指紋センサ１１と、作業用メモリ２５と、時刻データ２３を出力する時計２６と、赤外線送受光器２７と、プログラムおよび各種データを記憶する不揮発性メモリ２８と、電源供給の電池７と、カバーオープン検出回路８とから構成され、筐体（図示せず）に収容される。

【００４８】不揮発性メモリ２８として例えばフラッシュＲＯＭが使用され、ＣＰＵ１２の動作プログラム、指紋認証プログラム、公開鍵または秘密鍵のデータ、暗号化された指紋データ、認証結果のログ（記録）が格納されている。フラッシュＲＯＭは電源オフ状態でも格納したデータを保持するが、特別なプログラム操作で消去、書き換えが可能である。指紋センサ１１は指紋を指紋画像データとして数値化して読み込む。ＣＰＵ１２は指紋画像データをバス２９を介して作業用メモリ２５に蓄積してから、不揮発性メモリ２８の指紋認証プログラムを起動する。ここで暗号化された指紋画像データを公開鍵１９で復号し、作業用メモリ２５に予め蓄積した指紋画像データと比較する。

【００４９】この比較結果は認証されても認証されなくても、時計２６の時刻データとともに暗号化されて認証結果のログとして不揮発性メモリ２８に記録される。赤外線送受光器２７経由で、登録装置３０からの要求が有れば、認証結果のログの送信、指紋画像データの更新、公開鍵の更新等を行う。

【００５０】なお、外部電源（図示せず）が切断されると指紋認証は行わないが、一定時間動作する電池７により電力を供給する。筐体のカバーが開けられた場合、カバーオープン検出回路８が作動し、カバーオープンを示すカバー検出信号９をＣＰＵ１２に出力する。ＣＰＵ１

２は、外部電源が切断されていても電池７で動作できるので、不揮発性メモリ２８の公開鍵データを消去することができる。このため、公開鍵データの漏洩を防ぐことができる。

【００５１】なお、認証装置１０と登録装置３０との通信は赤外線送受光部１６，３３による赤外線通信に限定されるものではなく、イーサネットをもちいた通信でもよい。

【００５２】上述の通り、認証装置１０には暗号化された認証データ２０と公開鍵１９とが格納されているだけであるので、秘密鍵３７がないと復号できないため個人情報が安全に保護され、認証装置１０も簡単な構成で実現できる。

【００５３】

【発明の効果】以上説明したように、本発明の指紋認証システムは認証装置と登録装置とが分離しておりシステム構成を簡素化できるので、１台の登録装置で複数の認証装置を管理できるという効果を有している。

【００５４】認証装置には個人情報を格納せず暗号化された認証データのみを格納し、かつ認証データを生成する秘密鍵を有さないので、認証データの偽造を防止できるという効果を有している。

【００５５】また、認証装置と登録装置の通信は全て暗号化しているので、安全性を確保できるという効果を有している。

【図面の簡単な説明】

【図１】本発明の指紋認証システムの一つの実施の形態を示すブロック図である。

【図２】本発明の指紋認証システムの動作の一例を示す動作説明図である。

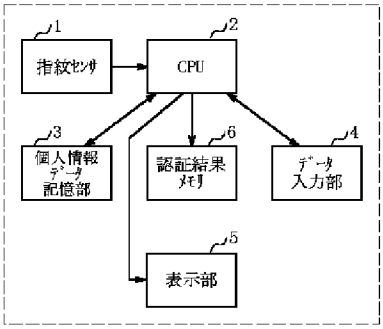
【図３】図１に示す認証装置の詳細ブロック図である。

【図４】従来の指紋認証システムを示すブロック図である。

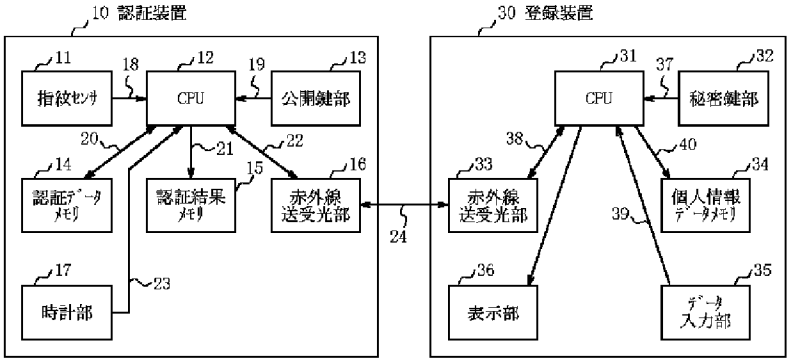
【符号の説明】

１　指紋センサ
２　ＣＰＵ
３　個人情報データ記憶部
４　データ入力部
５　表示部
６　認証結果メモリ
７　電池
８　カバーオープン検出回路
９　カバー検出信号
１０　認証装置
１１　指紋センサ
１２　ＣＰＵ
１３　公開鍵部
１４　認証データメモリ
１５　認証結果メモリ
１６　赤外線送受光部
１７　時計部
１８　指紋情報
１９　公開鍵
２０　認証データ
２１　照合データ
２２　認証登録指紋データ
２３　時刻データ
２４　赤外光
２５　作業用メモリ
２６　時計
２７　赤外線送受光器
２８　不揮発性メモリ
２９　バス
３０　登録装置
３１　ＣＰＵ
３２　秘密鍵部
３３　赤外線送受光部
３４　個人情報データメモリ
３５　データ入力部
３６　表示部
３７　秘密鍵
３８　認証データ
３９　個人情報
４０　個人情報データ

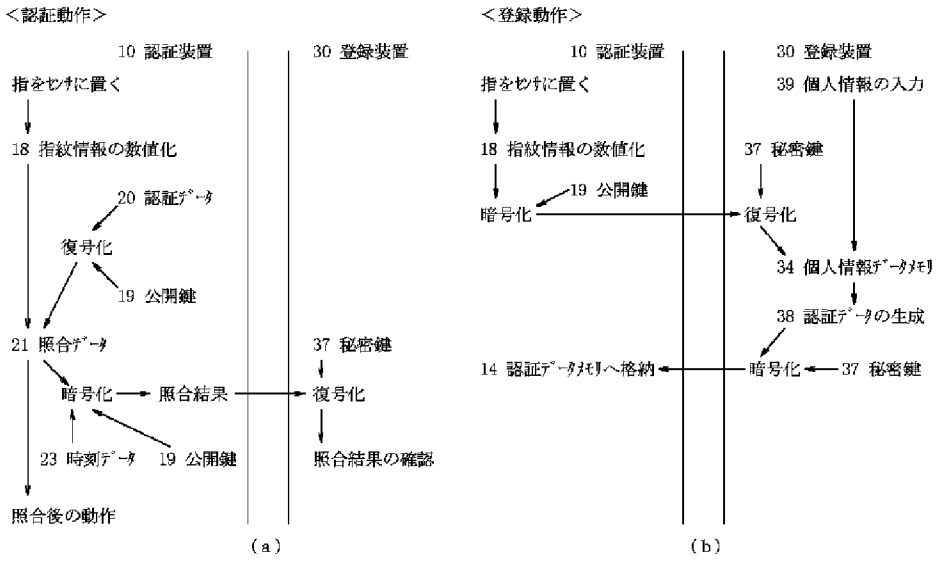
【図４】



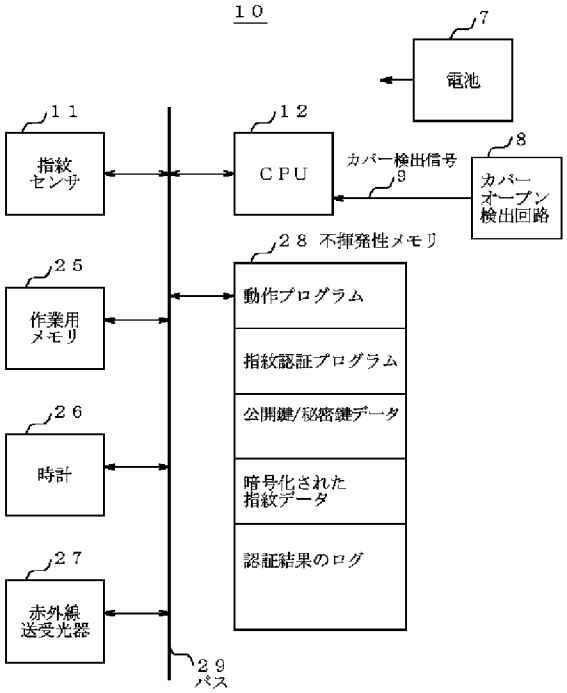
【図１】


10 認証装置
11
指紋ｾﾝｻ
18
12
CPU
19
13
公開鍵部
20
21
22
14
認証ﾃﾞｰﾀ
ﾒﾓﾘ
15
認証結果
ﾒﾓﾘ
16
赤外線
送受光部
24
17
時計部
23
30 登録装置
31
CPU
37
32
秘密鍵部
38
40
33
赤外線
送受光部
34
個人情報
ﾃﾞｰﾀﾒﾓﾘ
39
36
表示部
35
ﾃﾞｰﾀ
入力部

【図２】


＜認証動作＞
10 認証装置
30 登録装置
指をｾﾝｻに置く
18 指紋情報の数値化
20 認証ﾃﾞｰﾀ
復号化
19 公開鍵
21 照合ﾃﾞｰﾀ
37 秘密鍵
暗号化
照合結果
復号化
23 時刻ﾃﾞｰﾀ
19 公開鍵
照合結果の確認
照合後の動作
(a)
＜登録動作＞
10 認証装置
30 登録装置
指をｾﾝｻに置く
39 個人情報の入力
18 指紋情報の数値化
37 秘密鍵
19 公開鍵
暗号化
復号化
34 個人情報ﾃﾞｰﾀﾒﾓﾘ
38 認証ﾃﾞｰﾀの生成
14 認証ﾃﾞｰﾀﾒﾓﾘへ格納
暗号化
37 秘密鍵
(b)

【図３】


１０
７
電池
１１
指紋
センサ
１２
ＣＰＵ
カバー検出信号
９
８
カバー
オープン
検出回路
２８ 不揮発性メモリ
２５
作業用
メモリ
動作プログラム
指紋認証プログラム
公開鍵/秘密鍵データ
２６
時計
暗号化された
指紋データ
認証結果のログ
２７
赤外線
送受光器
２９
バス